Known issues in this release

- LAN-Modem profiles contain entries for 96 devices. For the 96-port MultiDSP card, all 96 entries in the profile are used. For 48-port modem cards (Series56 modem card (TNT-SL-48MOD-S56), Series56 II (TNT-SL-48MOD-S-C), and Series56 III (TNT-SL-48MODV3-S-C) cards), only the first 48 entries are used. For the 48-port MultiDSP card (TNTP-SL-ADI-C or TNTV-SL-ADI-C), every other entry in a LAN-Modem profile is used (odd ports only, from 1 to 95).
- Incompatibility with MultiVoice Access Manager Release 2.x.
  - Dynamic call control and multiple logical gateways are only supported in MultiVoice networks running TAOS Release 8.0-103 on the gateways and MVAM Release 3.0 on the gatekeepers. These features are not supported in MultiVoice networks where gatekeepers are running Release 2.x of the MultiVoice Access Manager.
  - New parameter definitions are added to the Non-Standard data messages (such as, trunk/DS0 reporting, non-standard call failure codes) sent by a MultiVoice Gateway to the MultiVoice Access Manager.
- Change in Call-logging packet format

  In releases prior to 7.2.0, the format of Call-logging packets are identical to RADIUS Accounting packets. With the introduction of 7.2.0, Call-logging will no longer be compatible with RADIUS, although Lucent's NavisAccess product fully supports MultiVoice Call-logging. The MAX TNT continues to support RADIUS accounting, SNMP and SYSLOG functionality.

  Because of the proprietary nature of and potential modification to call-logging packets, you should not use call-logging packets with any application other than Lucent's NavisAccess.

Upgrade and downgrade procedures

This section shows how to upgrade and downgrade the TAOS software of a MAX TNT unit.

Note: Digital subscriber loop (DSL) functionality is not supported in this release. See "Notice of discontinuance of MAX TNT support for DSL" on page 14.

Requirements and recommendations

These recommendations for upgrading MAX TNT units help ensure a smooth upgrade. If you must downgrade from this release to a previous one, please see "Downgrade instructions" on page 6.

Obtaining the MAX TNT TAOS 8.0-103 software

The MAX TNT TAOS 8.0-103 software consists of the following files:

Filename	Descriptions
`tntsrb.bin`	The boot loader. Both T1 and E1 loads use the same boot loader software. Lucent recommends that you always install a new boot loader when upgrading to a release.
`tntrel.tar`	Tar file (T1 load) that contains images for the shelf controller and all MAX TNT slot cards.
`tntrele.tar`	Tar file (E1 load) that contains images for the shelf controller and all MAX TNT slot cards.

You can obtain the files you need from the anonymous FTP server ftp.ascend.com. If you need technical assistance, see "Customer Service" on page 3.

Local access to the unit recommended

Whenever you install system software, Lucent recommends that you access the unit through the shelf controller serial or LAN port rather than a slot card port.

32-MB JEDEC DRAM card required for this release

For this release, the MAX TNT requires a 32-MB JEDEC DRAM card (model number TNT-SP-DRAM-32). New MAX TNT units now ship standard with the 32-MB DRAM card.

The 32-MB JEDEC DRAM card is *not* hot swappable. To install the card, you must turn off power to the MAX TNT, insert the card and then power on the MAX TNT. For additional information about the card, contact your service representative.

Flash size limitations for this upgrade

Because the MAX TNT supports many different slot card types, the tar files containing slot-card code images can be too large to load on an 8-MB flash card. TAOS 7.0.0 introduced a new

S 889

Load-Select profile type that prevents loading the entire set of slot-card images. The profile causes the system to determine which card types are present and load only those images. For details about the Load-Select profile, see the *MAX TNT Reference Guide*.

In addition, in this release, the `tntbase.tar` and `tntbasee.tar` files are less than 8-MB in size and are guaranteed to fit on an 8-MB flash card.

If neither of the small tar files are appropriate for your systems, to load this release to 8MB flash, make sure that all parameters in the Load-Select profile are set to `auto` and that the combined binaries required to run the system and its cards do not exceed 8MB. Following are the approximate sizes of each binary in the tar file:

Table 1. Approximate sizes of shelf controller and card binaries

System component	Binary filename	Approx. size (KB)
Shelf controller (T1)	`tntsr/tntsr.ffs`	1800
Shelf controller (E1)	`tntsre/tntsre.ffs`	1800
8T1	`tnt8t1/tnt8t1.ffs`	275
UTI (Frameline)	`tntut1/tntut1.ffs`	825
8E1	`tnt8e1/tnt8e1.ffs`	260
UE1 (E1 Frameline)	`tntue1/tntue1.ffs`	810
T3	`tntt3/tntt3.ffs`	310
Ethernet-2	`tntenet2/tntenet2.ffs`	240
Ethernet-3	`tntenet3/tntenet3.ffs`	355
HDLC-2	`tnthdlc2/tnthdlc2.ffs`	1005
HDLC-2EC	`tnthdlc2ec/tnthdlc2ec.ffs`	1000
SWAN	`tntswan/tntswan.ffs`	725
UDS3	`tntuds3/tntuds3.ffs`	730
DS3-ATM	`tntds3atm/tntds3atm.ffs`	735
OC3-ATM	`tntoc3atm/tntoc3atm.ffs`	730
Analog modem	`tntamdm/tntamdm.ffs`	700
56K modem	`tntmdm56k/tntmdm56k.ffs`	850
Series56 I/ Series56 II	`tntcsmx/tntcsmx.ffs`	990
Series56 III	`tntcsm3v/tntcsm3v.ffs`	980
MultiDSP	`tntmadd/tntmadd.ffs`	1300
STM-0	`tntstm0/tntstm0.ffs`	300

Saving the system configuration

As a general practice, always save the system configuration before upgrading or downgrading system software. You can then restore the configuration along with earlier system software if anything unexpected occurs during the upgrade or downgrade. If you use TFTP to save the system configuration, the target file must exist on the TFTP server and you must have permission to write it. For example, the following commands executed on a TFTP server create a target file and set its permissions:

```
$ touch /tftpboot/config/testcfg.1
```

```
$ chmod a=rw /tftpboot/config/testcfg.1
```

Before you save the system configuration, you must enable the Allow-Password permission in the MAX TNT User profile to save the configured passwords. If you do not have Allow-Password permission enabled, you will be prompted to confirm that you wish to save the configuration without passwords. If you do so and then restore the saved configuration, all passwords in the configuration are wiped out. The following commands executed on the MAX TNT save the system's configuration to the target file on the TFTP server and then restore the saved configuration:

```
admin> save -a network 10.10.10.10 /tftpboot/config/testcfg.1
admin> load config network 10.10.10.10 /tftpboot/config/testcfg.1
```

Upgrade instructions

These instructions show how to upgrade to MAX TNT TAOS 8.0-103 from TAOS version 7.0.0 or later. If you are not sure which version the system is running, enter the `version` command. For example:

```
admin> version
Software version 7.2.0
```

If the system is running a software version earlier than 7.0.0, please upgrade to 7.0.0 first and then follow the instructions in this note. For information about upgrading to 7.0.0, you can access the MAX TNT TAOS 7.0.0 release note at http://www.ascend.com/doclibrary.

Note: Under certain conditions, the `load tar` command might recognize no slot cards and load only the shelf controller image during the upgrade procedure. If this occurs, reset the system and load the tar file again. The second `load tar` command will load the appropriate slot-card images for the system.

If you are upgrading from MAX TNT TAOS 7.0V

MAX TNT TAOS 8.0-103 introduces a DOS-compatible general-purpose file system. If you are upgrading to MAX TNT TAOS 8.0-103 from a TAOS 7.0V release and you intend to use the new file system format, you must first reformat the flash card to the old format. This is required. For example:

```
admin> format -o flash-card-1
```

After formatting the flash card to the old format, follow the upgrade instructions in the next section or in "Upgrading a multishelf MAX TNT unit" on page 4.

The initial format operation erases the card's contents, including all voice announcements stored on the card. When the upgrade is complete, you must reload the voice announcements. For example, the following command loads a voice-announcement file named `busy.au` from a TFTP server at 10.10.10.10 to the `/current` directory on flash card 1 (flash card 1 is the default):

```
admin> load file network 10.10.10.10 busy.au
```

For more information details about loading voice announcements, see "Storing voice announcements in the FAT-16 flash memory file system" on page 268.

S 891

Upgrading a standalone MAX TNT unit

To upgrade a standalone unit with 8MB flash, proceed as follows:

1. Log into the system and save its configuration to a TFTP server. This step is optional but strongly recommended. For details, see "Saving the system configuration" on page 2.
2. Verify that the combined binaries required to run the system and its cards do not exceed 8MB. See "Approximate sizes of shelf controller and card binaries" on page 2.
3. Verify that the Load-Select profile is configured to automatically load only required binaries. All parameters in the profile must be set to `auto`.
4. Format the flash card. For example:
   ```
   admin> format flash-card-1
   ```
5. Load the boot loader. For example:
   ```
   admin> load boot-sr network 10.10.10.10 tntsrb.bin
   ```
6. Load the tar file. For example:
   ```
   admin> load tar network 10.10.10.10 tntrel.tar
   ```
7. Reset the system. This step is required. For example:
   ```
   admin> reset
   ```
8. Telnet into the system via the serial connection. Verify that the shelf controller IP address is set. For example:
   ```
   admin> get ip-interface { { 1 c 1 } 0} ip-address
   [in IP-INTERFACE/{ { shelf-1 controller 1 } 0 }:ip-address]
   ip-address = 10.10.10.2/24
   ```
   If the address is not set, open the IP-Interface profile for the shelf controller and set the address. For example:
   ```
   admin> read ip-interface { { 1 c 1 } 0}
   IP-INTERFACE/{ { shelf-1 controller 1 } 0 } read

   admin> set ip-address = 10.10.10.2/24

   admin> write
   IP-INTERFACE/{ { shelf-1 controller 1 } 0 } written
   ```
9. Load the system configuration. This step is optional, but recommended. For example:
   ```
   admin> load config network 10.10.10.10 /tftpboot/config/tntconfig
   ```
10. Format the flash card again. For example:
    ```
    admin> format flash-card-1
    ```
11. Load the tar file again. For example:
    ```
    admin> load tar network 10.10.10.10 tntrel.tar
    ```
12. Reset the system. This step is optional, but recommended. For example:
    ```
    admin> reset
    ```

Upgrading a multishelf MAX TNT unit

If you are upgrading a multishelf system, you must propagate the new boot loader to the slave shelves by using the Loadslave command. (The version of the `tntsrb.bin` file on the master shelf must match the `tntsrb.bin` version on the slave shelves. Otherwise, the slave shelves cannot load code from the master shelf.) In addition, you must propagate a link to a redundant image of the tar file located in onboard flash.

To upgrade a multishelf unit with 8MB flash, proceed as follows:

1. Log into the master shelf and save the configuration to a TFTP server. This step is optional but strongly recommended. For details, see "Saving the system configuration" on page 2.
2. Verify that the combined binaries required to run the system and its cards do not exceed 8MB. See "Approximate sizes of shelf controller and card binaries" on page 2.
3. Verify that the Load-Select profile is configured to automatically load only required binaries. All parameters in the profile must be set to `auto`.
4. Format the flash card. For example:

   ```
   admin> format flash-card-1
   ```
5. Load the boot loader. For example:

   ```
   admin> load boot-sr network 10.10.10.10 tntsrb.bin
   ```
6. Propagate the new boot loader to the slave shelves. For example, the following command propagates the boot loader to a slave shelf with a rotary-switch setting of 2:

   ```
   admin> loadslave 2 boot-sr
   ```
7. Load the tar file. For example:

   ```
   admin> load tar network 10.10.10.10 tntrel.tar
   ```
8. Reset the system. This step is required. For example:

   ```
   admin> reset -a
   ```
9. Telnet into the system via the serial connection. Verify that the master shelf controller IP address is set. For example:

   ```
   admin> get ip-interface { { 1 c 1 } 0} ip-address
   [in IP-INTERFACE/{ { shelf-1 controller 1 } 0 }:ip-address]
   ip-address = 10.10.10.2/24
   ```

   If the address is not set, open the IP-Interface profile for the shelf controller and set the address. For example:

   ```
   admin> read ip-interface { { 1 c 1 } 0}
   IP-INTERFACE/{ { shelf-1 controller 1 } 0 } read

   admin> set ip-address = 10.10.10.2/24

   admin> write
   IP-INTERFACE/{ { shelf-1 controller 1 } 0 } written
   ```
10. Load the system configuration. This step is optional, but recommended. For example:

    ```
    admin> load config network 10.10.10.10 /tftpboot/config/tntconfig
    ```
11. Format the flash card again. For example:

    ```
    admin> format flash-card-1
    ```
12. Load the tar file again. For example:

    ```
    admin> load tar network 10.10.10.10 tntrel.tar
    ```
13. Use the Loadslave command to propagate a link to the `image2` file, which is a redundant image of the tar file created in onboard flash. For example, the following command propagates the image to a slave shelf with a rotary-switch setting of 2:

    ```
    admin> loadslave 2 image2
    ```
14. Reset the system. This step is optional, but recommended. For example:

    ```
    admin> reset -a
    ```

Downgrade instructions

Because releases are not necessarily backward compatible, Lucent recommends that you always restore a backup configuration made under the previous version or one of its predecessors.

If you have enabled extended profiling and then must downgrade to an earlier software version, see "Additional onboard memory for extended profiling" on page 92, for important information.

> **Note:** Serial access to the MAX TNT unit is required for downgrading to a previous release from MAX TNT TAOS 8.0-103. Because of the new profiles and functionality introduced in MAX TNT TAOS 8.0-103, you must initialize the system by clearing the onboard nonvolatile random access memory (NVRAM) when performing a downgrade. When you clear NVRAM, the initialized system starts up unconfigured, just as it was when you first installed it, with no IP address assignments.

Downgrading a standalone MAX TNT unit

To restore an earlier system software version, proceed as follows:

1. Log into the MAX TNT and save the current configuration to a TFTP server. This step is optional, but recommended.
2. Reformat the flash card to the old format. This is required. For example:
   ```
   admin> format -o flash-card-1
   ```
3. Load the previous version of the boot loader. For example:
   ```
   admin> load boot-sr network 10.10.10.10 tntsrb.bin
   ```
4. Load the previous version of the tar file. For example, to load via TFTP from a local host:
   ```
   admin> load tar network 10.10.10.10 tntrel.tar
   ```
5. Clear NVRAM. This step is required when downgrading. For example:
   ```
   admin> nvram -f
   ```
6. Telnet into the system via the serial connection. Open the IP-Interface profile for the shelf controller and set the address. For example:
   ```
   admin> read ip-interface { { 1 c 1 } 0}
   IP-INTERFACE/{ { shelf-1 controller 1 } 0 } read

   admin> set ip-address = 10.10.10.2/24

   admin> write
   IP-INTERFACE/{ { shelf-1 controller 1 } 0 } written
   ```
7. Load a backup configuration made under the restored software version or one of its predecessors. For example:
   ```
   admin> load config network 10.10.10.10 /tftpboot/config/7x-config
   ```
8. Reset the system. This step is optional, but recommended. For example:
   ```
   admin> reset
   ```

Downgrading a multishelf MAX TNT unit

If you are downgrading a multishelf system, you must propagate the restored boot loader to the slave shelves by using the Loadslave command. (The version of the `tntsrb.bin` file on the master shelf must match the `tntsrb.bin` version on the slave shelves. Otherwise, the slave shelves cannot load code from the master shelf.) In addition, you must propagate a link to a redundant image of the restored tar file. To restore an earlier system software version, proceed as follows:

1 Log into the master shelf and save the current configuration to a TFTP server. This step is optional, but recommended.

2 Reformat the flash card to the old format. This is required. For example:

```
admin> format -o flash-card-1
```

3 Load the previous version of the boot loader. For example:

```
admin> load boot-sr network 10.10.10.10 tntsrb.bin
```

4 Propagate the boot loader to the slave shelves. For example, the following command propagates the boot loader to a slave shelf with a rotary-switch setting of 2:

```
admin> loadslave 2 boot-sr
```

5 Load the previous version of the tar file. For example, to load via TFTP from a local host:

```
admin> load tar network 10.10.10.10 tntrel.tar
```

6 Clear NVRAM. This step is required when downgrading. For example:

```
admin> nvram -f
```

7 Telnet into the system via the serial connection. Open the IP-Interface profile for the shelf controller and set the address. For example:

```
admin> read ip-interface { { 1 c 1 } 0}
IP-INTERFACE/{ { shelf-1 controller 1 } 0 } read

admin> set ip-address = 10.10.10.2/24

admin> write
IP-INTERFACE/{ { shelf-1 controller 1 } 0 } written
```

8 Load a backup configuration made under the restored software version or one of its predecessors. For example:

```
admin> load config network 10.10.10.10 /tftpboot/config/7x-config
```

9 Use the Loadslave command to propagate a link to the `image2` file, which is a redundant image of the tar file created in onboard flash. For example, the following command propagates the image to a slave shelf with a rotary-switch setting of 2:

```
admin> loadslave 2 image2
```

10 Reset the system. This step is optional, but recommended. For example:

```
admin> reset -a
```

MultiVoice features in MAX TNT TAOS 8.0-103

Modem manager

Firmware versions for digital modems

The Conexant firmware versions for MAX TNT Digital Modem cards include support for V.90, K56flex, K56plus, and all slower, standard modem speeds. This release includes the following Conexant firmware:

- Series56 Digital Modem cards (also called CSM/1, TNT-SL-48MOD-S56) support V2.0982-K56_2M_DLP_CSM firmware.
- Series56 II Digital Modem cards (also called CSM/3, TNT-SL-48MOD-SGL and TNT-SL-48MOD-S-C) support V5.817 firmware.
- Series56 III Digital Modem cards (also called CSM/3V, TNT-SL-48MODV3-S-C) support V5.8173 firmware.

The V5.817 and V5.8173 firmware include a fix for synchronization rate failures with some PCtel chipset modems. The V5.8173 firmware also provides a fix for synchronization failures observed with some Lucent winmodems.

Firmware versions for MultiDSP cards

This release includes the following Lucent firmware versions for MultiDSP cards:

- 48-port MultiDSP cards (TNTP-SL-ADI-C or TNTV-SL-ADI-C) support Lucent V0.1614.1 firmware.
- 96-port MultiDSP cards (APX8-SL-96DSP) support Lucent V0.1614.1 firmware.

Series56 III modem card support

The Series56 III Digital Modem card (TNT-SL-48MODV3-S-C) is a single-slot 48-port card that is the functional equivalent of the Series56 II card. Ongoing support continues in parallel for the Series56, Series56 II, and Series56 III modules.

The new Series56 III has the same installation and configuration procedures as the Series56 II card, described in the *MAX TNT Hardware Installation Guide*. The procedures are also described in the Series56 II guide, which you can access online after registering at http://www.ascend.com/doclibrary.

The output of the Show command identifies the Series56 III Digital Modem card as `csmv-card`, as shown in the following example:

```
admin> show
 Shelf 1 ( standalone ):
    { shelf-1 slot-14 0 }      UP       csmv-card
```

Expanded MultiDSP card support

In addition to the 48-port MultiDSP card (TNTP-SL-ADI-C or TNTV-SL-ADI-C) a 96-port MultiDSP card (APX8-SL-96DSP) is now available.

Modem service is now supported and enabled by default on both MultiDSP cards.

With the appropriate software licenses, services currently supported on the 48-port MultiDSP card are: modem (for example, V.90), ISDN (HDLC), V.110, PHS, and VoIP (voice). The 96-port card does not support PHS or VoIP in this release.

PHS functionality now supports a fixed data rate of 32Kbps (PIAFS 1.0), or a fixed data rate of either 32Kbps or 64Kbps for the duration of a call (PIAFS 2.0), or a data rate that switches between 32Kbps and 64Kbps during a call, depending on what the wireless bandwidth permits (PIAFS 2.1). The PIAFS 2.1 functionality requires a separate license

The 48-port MultiDSP card supports 48 ports of any service and handles up to two different services per card. In this release, when running two services per card, the services can be used only in one of the following combinations:

- Data (modem/ISDN) with V.110
- Data (modem/ISDN) with PHS
- Data (modem/ISDN) with VoIP

The 96-port MultiDSP card currently supports 96 ports of data (modem/ISDN) and/or V.110 service, and handles up to two different services per card. When running two services per card, one service must be data and the other must be V.110. The 96-port card does not support PHS or VoIP in this release.

In this release, the following configuration restrictions apply:

- The 96-port and 48-port MultiDSP card cannot be used together in the same unit.
- The dual-port Series56 card (TNT-SL-48MOD-S56) cannot be used in the same unit with MultiDSP cards.

Multiple 48-port MultiDSP cards can be used in the same unit, and the Series56 II (TNT-SL-48MOD-SGL and TNT-SL-48MOD-S-C) and Series56 III (TNT-SL-48MODV3-S-C) cards can be used in the same unit as a MultiDSP card.

For further details on the MultiDSP cards, see the MultiDSP guide at http://www.ascend.com/doclibrary. After you register, you can view or download the guide.

MultiVoice operations

Support for MultiVoice operations was introduced with limited availability in earlier TAOS 7.x releases, and was made generally available in MAX TNT TAOS 8.0.2. This *Limited Availability Release* contains new features and corrections introduced in the True Access™ Operating System (TAOS) for the MAX TNT™, supporting the MultiVoice feature set.

MultiVoice functionality includes Voice over IP (VoIP) and a transparent data mode that enables users to run a modem on a VoIP channel. With a separate license on both ends of the transmission, MultiVoice also supports real-time fax over IP.

Note: This release note provides an overview of MultiVoice functionality and describes new MAX TNT TAOS 8.0-103 features that are not documented in the *MultiVoice for the MAX TNT Configuration Guide*. For details about MultiVoice configuration, see the guides at http://www.ascend.com/doclibrary.

In MAX TNT TAOS 8.0-103, the following MultiVoice software licenses can be enabled:

- VoIP, which enables the MAX TNT to act as an H.323v2 MultiVoice Gateway for transmission of real-time voice calls and transparent modem calls across IP networks.
- VoIP and SS7, which enables the MAX TNT to act as a MultiVoice Gateway that communicates with an SS7 signaling gateway to transmit real-time voice calls and transparent modem calls from an SS7 network across IP networks.
- Real-time fax (T.38) over IP, which uses the VoIP framework for call establishment, fax detection, and fax initiation.

For information about using MultiVoice for basic long-distance service and 800 service, and with overlapping coverage areas and multizone call routing, see the *MultiVoice for the MAX TNT Configuration Guide* at http://www.ascend.com/doclibrary.

System requirements for VoIP

To operate as a MultiVoice Gateway, a MAX TNT unit must have the following equipment and licenses:

- VoIP software licenses
- Sufficient MultiDSP cards to process VoIP calls
- Sufficient T1, T3, or E1 trunks to process VoIP calls
- Sufficient Ethernet-3 cards to process VoIP calls

If the MAX TNT unit will operate in an H.323 environment, it must also have an IP connection to a workstation running the MultiVoice Access Manager (MVAM) software.

If the unit will operate in an SS7 environment, the SS7 software license must also be enabled so that the system can perform IPDC packet processing.

Ethernet requirements for VoIP processing

MAX TNT units do not support routing of VoIP calls through the shelf controller Ethernet port. Ethernet-3 (TNT-SL-E100-V-C) cards are required for VoIP. The Ethernet-3 card is a high performance Ethernet module with one 100-MB interface designed for demanding applications such as VoIP.

Full-duplex mode required

When using the Ethernet-3 card to support VoIP call processing, the card must operate in full-duplex mode. The card operates in full-duplex mode by default, as specified in the setting of the following parameter:

```
[in ETHERNET/{ any-shelf any-slot 0 }]
duplex-mode = full-duplex
```

Compatible configuration in connecting port of hub or router

The 100-MB interface on the Ethernet-3 card is not autoconfigurable and Lucent does not recommend connecting it to a hub or router port that has been autoconfigured. Connecting it to an autoconfigured port can have negative effects on VoIP calls, including poor voice quality for connected calls and increased instances of initial call failures.

To ensure the best performance and quality for VoIP calls, make sure that the hub or router port that connects the Ethernet-3 card to the packet network complies with the following recommended configuration:

- Port autoconfiguration must be disabled.
- Port speed must be configured to operate at 100 Mbits only.
- Port must be configured for full-duplex transmission

Please refer to the manufacturer-provided documentation for your particular network hub, router or switch for specific instructions on configuring its Ethernet ports.

Note: It is not necessary to apply the recommended configuration to ports providing the outbound connection from the hub or router to the rest of the IP network. This configuration is required only for the port connecting to the Ethernet-3 card.

Overview of VoIP call routing

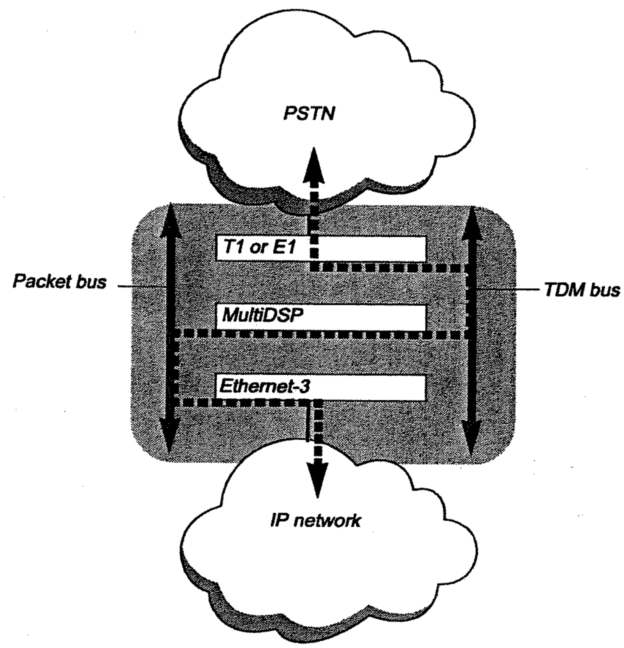
When a VoIP license has been enabled, the system creates a new Call-Route profile for each installed MultiDSP card that supports VoIP. The new Call-Route profile sets the Call-Route-Type parameter to `voip-call-type`, as shown in the following sample profile for a MultiDSP card in shelf 1, slot 3:

```
admin> get call-route { { { 1 3 0 } 0 } 3 }
[in CALL-ROUTE/{ { { shelf-1 slot-3 0 } 0 3 }]
index* = { { { shelf-1 slot-3 0 } 0 } 2 }
trunk-group = 0
phone-number = ""
preferred-source = { { any-shelf any-slot 0 } 0}
call-route-type = voip-call-type
```

The `voip-call-type` setting enables the system to route VoIP calls to the MultiDSP card. When the MAX TNT receives a VoIP call on a network line (such as T1 or E1), it routes the traffic internally on its time-division multiplex (TDM) bus to the MultiDSP card, which handles VoIP-related functions such as audio coder/decoder (codec) processing, RTP and UDP processing, and so forth.

The MultiDSP card then forwards the packetized traffic on the system's packet bus to an exit (egress) interface such as Ethernet or another T1 line. The example path shown in Figure 1 provides a simplified picture of how VoIP calls are routed through the MAX TNT.

Figure 1. Simplified view of VoIP call routing within the MAX TNT



For details about VoIP call routing and how to fine tune it, see the *MultiVoice for the MAX TNT Configuration Guide* at http://www.ascend.com/doclibrary.

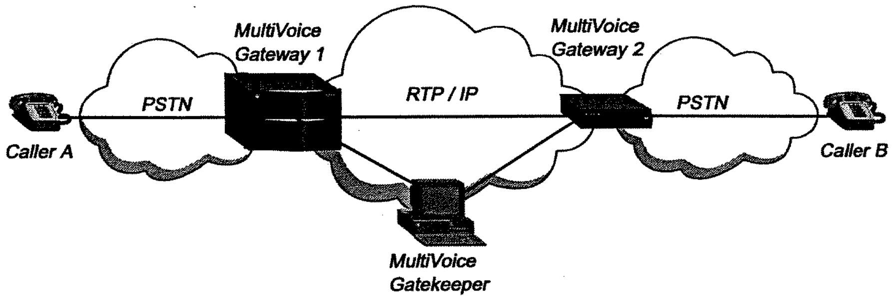
Overview of VoIP in an H.323v2 environment

MultiVoice is compliant with the ITU-T H.323 standard for the transmission of real-time voice communications across IP networks. H.323 systems use the IETF standard Real-Time Transport Protocol (RTP) with codecs for voice and other communications over the Internet.

VoIP-enabled MAX TNT units operate as MultiVoice Gateways. Callers dial into a local MAX TNT through the PSTN. The MAX TNT then communicates with a MultiVoice Gatekeeper to establish communication channels to a far end MultiVoice Gateway. Workstations running MVAM software operate as H.323 MultiVoice Gatekeepers, which handle all call control functions, including bandwidth control, authentication, call-detail recording (CDR), and alias translation.

In the example Gateway and Gatekeeper configuration in Figure 2, two Gateways connect Caller A to Caller B. A system running MVAM performs the H.323 Gatekeeper functions.

Figure 2. Example diagram of MultiVoice in H.323 environment



When Caller A dials Caller B, events such as the following occur:

1. Caller A dials Gateway 1, and enters his or her PIN authentication (if required) and Caller B's telephone number.
2. Gateway 1 establishes a session with the Gatekeeper, and then forwards the telephone number and PIN authentication to the Gatekeeper.
3. The Gatekeeper authenticates Caller A and, if authentication is successful, forwards the IP address of Gateway 2 to Gateway 1.
4. Gateway 1 establishes a session with Gateway 2.
5. Gateway 2 forwards the call request to Caller B.
6. When Caller B answers the telephone (goes off-hook), voice traffic is tunneled in IP packets by means of RTP, between Gateway 1 and Gateway 2.

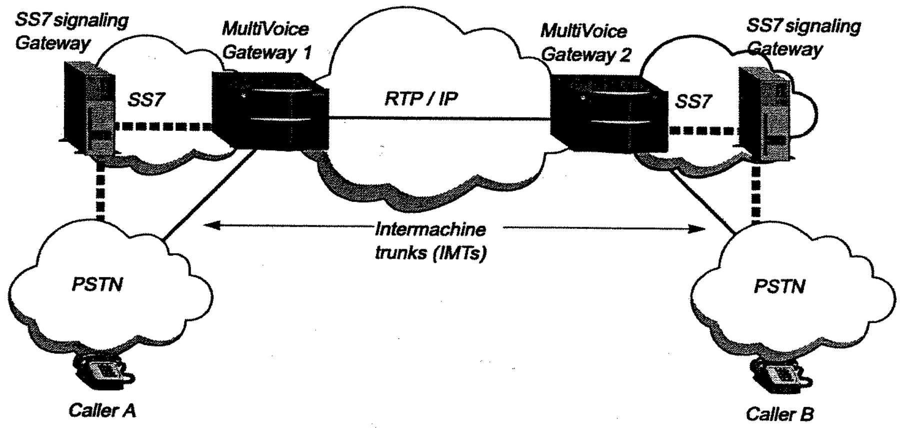
Overview of VoIP in an SS7 IPDC 0.12 environment

In an SS7 environment, VoIP-enabled MAX TNT units are MultiVoice Gateways that communicate with an SS7 signaling gateway to establish communication channels to a far-end MultiVoice Gateway.

The SS7 signaling gateways initiate and manage call setup and release, and execute call routing. The signaling gateway communicates call setup information to the MAX TNT using IPDC 0.12. IPDC message tags define voice encoding type, packet loading, IP and RTP ports, and other variables used for processing VoIP calls

In the example MultiVoice Gateway and signaling gateway configuration in Figure 3, the Gateways support VoIP calls controlled by IPDC over intermachine trunks (IMTs) for SS7 calls originating from the PSTN.

Figure 3. Example diagram of MultiVoice in SS7 environment



When Caller A dials Caller B, the following events occur:

1. Caller A dials the number for their SS7 service provider plus Caller B's telephone number. For example, Caller A dials a number such as 10-10-999-1-888-555-1212.
2. The signaling gateway assembles call routing information, and other information required to connect the call, such as user authentication and call reporting information.
3. The signaling gateway then sends an SS7 message to the PSTN to ring Caller B's telephone.
4. The signaling gateway uses IPDC to initiate an RTP/IP connection across the packet network between Gateway 1 and Gateway 2. The signaling gateway simultaneously sends IPDC setup information to both Gateway 1 and Gateway 2.
5. When Caller B answers the telephone (goes off-hook), the signaling gateway converts the SS7 signals into IPDC packets, and voice traffic is tunneled in IP packets between Gateway 1 and Gateway 2 by means of RTP.
6. Gateway 2 passes the IPDC packets to the signaling gateway at the far end, which converts the IPDC packets to SS7 messages and routes the call across the appropriate signaling links to Caller B.

In an SS7 environment, values in IPDC message tags override corresponding call management settings in the default VoIP profile.

General system configuration for VoIP support

Lucent recommends certain IP and call-handling configurations for processing VoIP calls. Global settings that are required for VoIP communication are also described in this section.

Note: For details about recommended IP settings and routes, see the *MultiVoice for the MAX TNT Configuration Guide* at http://www.ascend.com/doclibrary.

Disabling ICMP Destination Unreachable packets for VoIP calls

For Voice over IP (VoIP) calls, UDP for-me packets can arrive at a rate of 200 packets per second for each direction of each call. If the MAX TNT is not listening on a port for the for-me packets while setting up or tearing down a call, it returns ICMP Destination Unreachable

packets at the same rate. To prevent the performance penalty caused by this situation, you can now configure the system not to send ICMP Destination Unreachable packets.

Caution: This feature is intended only for VoIP environments. Enabling this feature can break required behavior for IPv4 routers, such as Path MTU Discovery.

Following is the relevant parameter, shown with its default setting:

```
[in IP-GLOBAL]
send-icmp-dest-unreachable = yes
```

Parameter	Specifies
Send-ICMP-Dest-Unreachable	Enable/disable sending of ICMP Destination Unreachable packets. The default is `yes`. If set to `no`, the MAX TNT does not send ICMP Destination Unreachable packets. Setting this parameter to No is recommended only for VoIP environments.

The following commands disable transmission of ICMP Destination Unreachable packets:

```
admin> read ip-global
IP-GLOBAL read

admin> set send-icmp-dest-unreachable = no

admin> write
IP-GLOBAL written
```

Preventing receipt of UDP packets until VoIP calls are set up

When two MultiVoice Gateway systems are establishing the link for transmission of a VoIP call, both systems do not always complete the call setup at the same time. However, a Gateway starts sending UDP packets to the other Gateway as soon its own call setup is complete. If the receiving Gateway has not yet set up its port caches, the shelf controller receives the UDP packets for a period of time until the call is fully set up. Now, you can prevent receipt of UDP packets until the link is fully established. Following is the relevant parameter, shown with the default value:

```
[in IP-GLOBAL]
throttle-no-port-match-udp-traffic-on-slot = no
```

Parameter	Specifies
Throttle-No-Port-Match-UDP-Traffic-On-Slot	Enable/disable reception of UDP packets for UDP ports currently unknown to the MAX TNT. With the default value of `no`, the system behaves as in previous releases and sends the unknown port packets to the shelf controller for processing. If the parameter is set to `yes`, the system discards UDP packets until the UDP port is known. The setting of `yes` is recommended for MultiVoice Gateways, to prevent overloading of the shelf controller when both Gateways do not always complete the VoIP call setup at the same time.

The following commands enable the system to discard UDP packets until the UDP port is known:

```
admin> read ip-global
IP-GLOBAL read
```

```
admin> set throttle-no-port-match-udp-traffic-on-slot = yes
admin> write
IP-GLOBAL written
```

System settings for VoIP operations

Lucent recommends setting the following parameters, shown with default values, to facilitate VoIP call handling:

```
[in IP-GLOBAL]
system-ip-addr = 0.0.0.0
[in ANSWER-DEFAULTS:session-info]
idle-timer = 0
[in SYSTEM]
max-dialout-time = 60
parallel-dialing = 32
country = us
```

Parameter	Recommended VoIP settings
System-IP-Addr	In an H.323 environment, set this parameter to the shelf controller IP address. In an IPDC environment, if the system allocates its own listen address, set this parameter to the IP address of a LAN interface other than the shelf controller port.
Idle-Timer	For real-time fax or transparent modem calls, set this parameter should be set to 0 to disable the idle timer and prevent the fax or modem calls from timing out.
Max-Dialout-Time	To allow sufficient time for the MAX TNT to establish the connection to the called destination, and for consistency with internal H.323 timers, a setting of 60 is recommended.
Parallel-Dialing	To decrease the instances when VoIP callers wait for a silent interval while the MAX TNT completes a call that has been queued, a setting of 32 is recommended.
Country	Setting this parameter to the appropriate value enables the MAX TNT to generate country-specific local call-progress tones (such as dial tone, busy signals, and so forth), based on the ITU-T specification TSB Circular 18: *Update of Supplement No. 2, ITU-T (former CCITT) Blue Book, Fascicle II.2 - Various tones used in national networks.* The following country-specific call progress tones are currently supported by MultiVoice: Argentina, Australia, Belgium, China, Costa Rica, Finland, France, Germany, Hong Kong, Italy, Japan, Korea, Mexico, Netherlands, New Zealand, Singapore, Spain, Sweden, Switzerland, United Kingdom, and the United States (the default).

For example, the following commands configure the system in a recommended way for VoIP call handling:

```
admin> read answer-defaults
ANSWER-DEFAULTS read
admin> set session-info idle-timer = 0
admin> write
ANSWER-DEFAULTS written
```

```
admin> read system
SYSTEM read

admin> set max-dialout-time = 60

admin> set parallel-dialing = 32

admin> set country = us

admin> write
SYSTEM written
```

Call route configuration

The MAX TNT Release 8.0-103 supports simultaneous processing of voice and data calls. To simplify routing of voice and data traffic between the MAX TNT and PSTN:

- Use DNIS-specific trunk mappings for detection of voice calls
- Process data and voice calls on different MultiDSP cards
- Use preferred source routing method (optional) for data call types
- Use trunk routing (optional) for outbound voice calls

Using DNIS-specific trunk mappings

The default VoIP profile, `voip { 0 0 }`, is a system-wide profile used for processing all VoIP calls. Additional VoIP profiles may be created to simplify processing and routing of VoIP calls.

User-defined VoIP profiles are used to map incoming calls by identifying all calls associated with a specific Dialed Number Identification Service (DNIS) string as VoIP calls. See "Creating user defined VoIP profiles" in the *MultiVoice for the MAX TNT Configuration Guide* for details.

Examples of user defined VoIP profiles

For example, if a user created the following VoIP profiles:

```
admin> dir voip
   46  12/23/1998 09:48:55  { 0 0 }
   31  12/18/1998 09:50:06  { 8093190 0 }
   31  12/18/1998 10:07:16  { 8903190 0 }
```

The MAX TNT will process all calls from the PSTN with these DNIS strings as VoIP calls. The Voip-Index subprofile distinguishes between the default VoIP profile, `voip { 0 0 }`, and any user created VoIP profiles:

```
admin> list voip-index
[in VOIP/{ 8903190 0 }:voip-index
gateway-access-number = 8903190
far-end-number = 0
```

This subprofile includes the following parameters:.

Parameter	Specifies
Gateway-Access-Number	This is the Dialed Number Identification String (DNIS) passed from the PSTN associated with the in-bound telephone number used to access the MAX TNT. If the MAX TNT is configured to perform two-stage dialing of VoIP calls, this would be the telephone number dialed to access the MAX TNT from the PSTN.
Far-End-Number	This value should always be set to `0`.

Note: This modification is made after the MAX TNT is initialized. Once these changes are committed, save the new configuration to flash memory or a tftp server. The saved image may be retrieved to restore this configuration in the event that a MAX TNT must be re-initialized.

Process voice and data calls on different MultiDSP cards

To enable the simultaneous processing of voice and data calls, you must create exclusive call routing types for each MultiDSP card. This is accomplished by deleting the Call-Route profiles for call types which should not be accepted for processing by a MultiDSP card.

At startup, up to four default Call-Route profiles are automatically created to handle different call types. Hash codes on the shelf controller determine which call route type profiles are created. The MAX TNT uses this profile to control which calls are accepted and processed by each MultiDSP card. Every possible destination within a MAX TNT system has one or more profiles of this type.

At least four types of Call-Route profiles are created for each installed MultiDSP card, as illustrated in the following `callroute` command output:

```
admin>callroute -d
device      #  source        type              tg  sa phone
1:03:01/0   1 0:00:00/0  digital-call-type     0   0
1:03:01/0   2 0:00:00/0  phs-call-type         0   0
1:03:01/0   3 0:00:00/0  voip-call-type        0   0
1:03:01/0   4 0:00:00/0  v110-call-type        0   0
```

The supported profile types for the MultiDSP card include:

Type	Description
Digital-Call-Type	General digital calls, including 3.1 Khz audio bearer channel calls can be routed to a device with this call route type. This is a host device. This Call-Route profile has an index of 1.
Phs-Call-Type	PHS calls can be routed to a device with this call route type. This Call-Route profile has an index of 2.
Voip-Call-Type	VOIP calls can be routed to a device with this call route type. This Call-Route profile has an index of 3.

S 906

Type	Description
V110-Call-Type	Digital calls recognized as containing V.110 rate adapted bearer channels cat be routed to device with this call route type. This Call-Route profile has an index of 4.

Depending upon whether the MultiDSP card will process voice or data calls, you should delete the call types as listed in the following:

For this default call type	Delete the following Call-Route profiles
VoIP calls (voip-call-type)	Any-Call-Type, Digital-Call-Type, V110-Call-Type
Data calls (digital-call-type)	Any-Call-Type, Voip-Call-Type

For example, if a MultiDSP card should only process VoIP calls, you would delete the Digital-Call-Type, V110-Call-Type and the Any-Call-Type profiles for the selected MultiDSP card.

Note: For all locations except Japan, the Phs-Call-Type Call-Route profile need not be deleted for MultiDSP cards processing voice calls. Currently, PHS calls are only supported by PSTNs in Japan.

To remove Call-Route profiles execute the following:

1 Use the `show` command to identify all the MultiDSP (`madd-card`) cards installed in your MAX TNT:

```
admin>show
Shelf 1 ( standalone ):
{ shelf-1 slot-1 0 }          UP        8e1-card
{ shelf-1 slot-2 0 }          UP        ether3-card
{ shelf-1 slot-3 0 }          UP        madd-card
{ shelf-1 slot-4 0 }          UP        madd-card
{ shelf-1 slot-5 0 }          UP        madd-card
{ shelf-1 slot-6 0 }          UP        madd-card
{ shelf-1 slot-7 0 }          UP        madd-card
{ shelf-1 slot-8 0 }          UP        madd-card
admin>
```

2 Delete the Call-Route profiles for each call type a MultiDSP card should not accept. To delete the Call-Route profile for V110-Call-Type processing on the MultiDSP slot card in slot 3, execute the following command:

```
admin> delete call-route { { {1 3 0} 0} 4}
Delete profile CALL-ROUTE/{ { { shelf-1 slot-3 0 } 0 } 4 }? [y/n] y

CALL-ROUTE/{ { { shelf-1 slot-3 0 } 0 } 4 } deleted

admin>
```

Repeat this procedure for each Call-Route profile associated with an excluded call type.

Note: This modification is made after the MAX TNT is initialized. Once these changes are committed, save the new configuration to flash memory or a tftp server. The saved image may be retrieved to restore this configuration in the event that a MAX TNT must be re-initialized.

Configuring preferred source routing

Using preferred source routing configures the MAX TNT to direct calls from the designated network device, (such as, T1 or E1 slot cards) to a specific MultiDSP card. This may be used to limit the calls a MultiDSP card accepts for processing to a specific T1 or E1 channel, and may be used for routing data calls.

This is accomplished by assigning the address of a T1 or E1 channel to the Preferred-Source parameter in the Call-Route profiles for each data call type configured for a MultiDSP card. This address identifies the shelf, slot, and connection associated with a specific T1 or E1 trunk.

To configure preferred source routing, execute the following:

1 Use the show command to identify all the T1 or E1 cards installed in your MAX TNT:

```
admin>show
Shelf 1 ( standalone ):
{ shelf-1 slot-1 0 }          UP        8e1-card
{ shelf-1 slot-2 0 }          UP        ether3-card
{ shelf-1 slot-3 0 }          UP        madd-card
{ shelf-1 slot-4 0 }          UP        madd-card
{ shelf-1 slot-5 0 }          UP        madd-card
{ shelf-1 slot-6 0 }          UP        madd-card
{ shelf-1 slot-7 0 }          UP        madd-card
{ shelf-1 slot-8 0 }          UP        madd-card
admin>
```

2 For each MultiDSP card, change the value assigned to the Preferred-Source parameter in the Call-Route profile for Digital-Call-Type. To route calls received through any E1 connected on slot 1 to the MultiDSP card in slot 4, execute the following command:

```
admin> read call-route { { {1 4 0} 0} 1}
CALL-ROUTE/{ { { shelf-1 slot-4 0 } 0 } 1 } read

admin>set preferred-source={{1 1 0} 0}

admin>write
CALL-ROUTE/{ { { shelf-1 slot-4 0 } 0 } 1 } written

admin>
```

You may configure a routing using all the T1 or E1 connections on the ingress card, as in the example, or specify an individual trunk by identifying a specific port on the ingress card, for example:

```
admin>set preferred-source={{1 1 4} 0}
```

Repeat this procedure until all T1 or E1 trunks are mapped to MultiDSP cards.

Note: This modification is made after the MAX TNT is initialized. Once these changes are committed, save the new configuration to flash memory or a tftp server. The saved image may be retrieved to restore this configuration in the event that a MAX TNT must be re-initialized.

Use trunk routing (optional) for outbound voice calls

Trunk routing of outbound VoIP calls is used to control allocation of T1 or E1 trunks for voice calls. The MAX TNT, which connects a VoIP call to the destination telephone number, can automatically route calls to the PSTN using a trunk group selected by the MAX TNT which initiated the call.

To utilize automated trunk routing:

- Trunk groups must be enabled on both MAX TNTs used to connect the call

S 908

- Both MAX TNTs should have the same number of T1 or E1 trunks available for connecting VoIP calls
- Both MAX TNTs must utilize the same trunk numbering scheme

When trunk prefixing is enabled, the MAX TNT obtains the trunk group number of the ingress T1 trunk from the `trunk-group` setting in the T1 line profile, and prefixes it to the detected DNIS, the destination telephone number. The MAX TNT modifies Q.931 Called Party Number information element (IE) in an H.225/Q.931 SETUP message, sending the DNIS number prefixed by the incoming trunk number to the MAX TNT which connects the voice call.

When the destination MAX TNT dials the call, it will connect the call to the PSTN using a trunk assigned to the requested trunk group.\

Enabling trunk groups

To enable automated trunk group processing of VoIP calls, you must configure the following:

Parameter	Profile	Value(s)	Description
Use-Trunk-Groups	System	Yes	This parameter enables the use of trunk groups for all network lines. When this parameter is enabled, all channels must be assigned a trunk group number for outgoing calls.
Num-Digits-Trunk-Groups	System	1- 4	This parameter sets a limit of the number of digits that may be used to designate trunk groups. The value assigned this parameter limits size of the values assigned to the Trunk-Group parameter to one- through four-place numbers.
Trunk-Group	T1 or E1	1 - 9999	This parameter assigns a channel to a trunk group. In a T1 or E1 profile, the default is 9. Individual channels may be assigned to different trunk groups.
Trunk-Prefix-Enable	Voip { x x }	Yes	This parameter enables outbound routing of VoIP calls over trunk groups from the ingress MAX TNT. The ingress MAX TNT will send the trunk group address as part of the dial string for the destination telephone number.

VoIP call management and performance settings

In an H.323 environment, settings in the default VoIP profile are used for processing all VoIP calls. In an SS7 environment, settings in the default VoIP profile are used only for settings that are not superseded by values in IPDC messages.

For details about VoIP profile settings that are new in MAX TNT TAOS 8.0-103, see *New VoIP profile settings in MAX TNT TAOS 8.0-103* on page 23.

New VoIP profile settings in MAX TNT TAOS 8.0-103

The following parameters (shown with default values) are new or modified in MAX TNT TAOS 8.0-103:

```
[in VOIP/{ 0 0 }]
gk-mlg-control = no
signaling-model = early-alerting

[in VOIP/{ 0 0 }:rt-fax-options]
packet-redundancy = no
fixed-packets = yes
max-rate = 9600
```

Parameter	Specifies
Gk-Mlg-Control	The Gk-Mlg-Control parameter enables the MultiVoice Gateway to accept and process call-specific administration instructions from a MultiVoice Access Manager, Release 3.0. When enabled, the gateway may apply call-specific processing instructions, for PIN authentication, single- or two-stage dialing, voice announcement playback, and configuring call timers for pre-paid billing. Values received from MVAM, or a third party billing system, will override parameter settings in the Voip { X X } profile for processing the current VoIP call. Rules used for performing call-specific administration are configured on MVAM, and are used when partitioning MultiVoice Gateways into multiple logical gateways. This allows MVAM to administer a single physical gateway as if it were multiple gateways, partitioning the gateway according to trunk groups, DNIS, time of day, etc.
Signaling-Model	This parameter controls processing of the H.245 startup procedure, by defining the relationship between H.323 alert messaging and PSTN alerting. This parameter creates a virtual inband pipeline for call signal processing by mapping PSTN actions into H.323 actions. When enabled, the H.245 startup information delivered in the Call Proceeding message provides for more transparent PSTN signaling behavior.
Packet-Redundancy	This parameter sets the packet redundancy scheme and jitter buffering for Multivoice Real-time fax over un-managed networks (such as, the public internet). When enabled, this parameter causes a MAX TNT to append the designated number of previously sent fax packets onto the current packet. On networks experiencing measurable packet loss, this improves the reliability of the fax transmission.
Fixed-Packets	This parameter lets customers disable the jitter buffer and packet redundancy scheme for Real-time fax calls. When packet redundancy is disabled, a MultiVoice Gateway running a pre-8.0-103 software release can process Real-time fax calls to and from a MultiVoice Gateway running the 8.0-103 software.

Parameter	Specifies
Max-Rate	This parameter sets the maximum data transmission rate allowed for a T.38 fax session configurable on a MultiVoice Gateway. This provides customers with a means to regulate the bandwidth used for fax sessions on their networks.

Configuring multiple logical gateways (MLG)

Using gatekeeper controlled multiple logical gateways is a method of performing call-specific administration of H.323 VoIP calls. The following call control functions may be used for partitioning one physical MultiVoice Gateway into multiple logical gateways from the gatekeeper:

- PIN prompting
- Single-stage dialing
- Two-stage dialing
- Voice announcement playback
- Configurable call timers for pre-paid and credit card billing systems

The MultiVoice Access Manager (MVAM) analyzes call performance data (trunk group, ds0 status and call activity), received when a gateway performs periodic keep-alive registration. When MVAM responds to subsequent call requests from each gateway, the Admission Conformation (ACF) message will include any changes defined for the aforementioned call administration parameters. The gateway applies the parameter changes received from MVAM to the current call request. This information is stored as part of the non-standard data included in registration, admission and status (RAS) messages exchanged by the gateway and gatekeeper for each call.

Warning: Dynamic call control and multiple logical gateways are only supported in Multi-Voice networks running TAOS Release 8.0-103 on the gateways and MVAM Release 3.0 on the gatekeepers. These features are not supported in MultiVoice networks where gatekeepers are running Release 2.x of the MultiVoice Access Manager.

Previously, all H.323 call management features were configured globally, on each MultiVoice Gateway, using the values assigned in the VOIP Options profile. Now, utilizing status information reported by MultiVoice Gateways, a gatekeeper running MultiVoice Access Manager, Release 3.0 may send instructions to the ingress gateway which override global call management settings. The decision to override the global call management settings may be based upon reported ingress trunk or DS0 groups, Caller ID, time-of-day, gateway, etc.

The rules used to apply overrides to H.323 call management parameters are configured on MVAM. These parameter changes are useful when partitioning MultiVoice Gateways into logical gateways. *Logical gateways*, defined on MVAM, treat selected trunk groups on a MultiVoice Gateway as if they were a unique VoIP gateway. Initially, MultiVoice Gateways must have T1, T3 and PRI trunks to support logical gateways. A MultiVoice Gateway won't know about its logical gateways, only MVAM does. However, a gateway must be configured to apply instructions received from MVAM when processing the current call.

Note: While BRI lines may still be used for VoIP, the multiple logical gateway features are not supported on MultiVoice Gateways using BRI.

S 911

MVAM may enable call-specific administration based upon the reported DNIS, ANI, trunk group and DS0 information, or any combination of that data, which are all reported in the first ARQ from the gateway.

Dynamic PIN authentication

When the multiple logical gateway feature is enabled on a MultiVoice Gateway, any incoming call request will immediately send an ARQ to MVAM which includes:

- DNIS, when available
- ANI, when available
- Trunk group and DS0 status changes

If the ARQ includes all the information necessary to route the call, MVAM will send an ACF message to the gateway. The gateway will then process the call as if the following VoIP parameters were set to these values:

```
vpn-mode=yes
single-dial-enable=yes
```

If MVAM, or a third party billing application used with MultiVoice, requires PIN authentication for this call, an Admission Reject (ARJ) message is issued directing the gateway to set `vpn-mode=no` for this call. The gateway will then resume call handling as if the call had just arrived from the PSTN, but prompt for authentication (as if `vpn-mode=no`) before continuing with call processing.

Dynamic single-stage and two-stage dialing

When the multiple logical gateway feature is enabled on a MultiVoice Gateway, any incoming call request will immediately send an ARQ to MVAM which includes:

- DNIS, when available
- ANI, when available
- Trunk group and DS0 status changes

If the ARQ includes all the information necessary to route the call, MVAM will send an ACF message to the gateway. The gateway will then process the call as if the following VoIP parameters were set to these values:

```
vpn-mode=yes.
single-dial-enable=yes
```

If MVAM, or a third party billing application used with MultiVoice, requires a caller perform two-stage dialing for this call (dialing the destination telephone number after dialing into the MultiVoice Gateway), an Admission Reject (ARJ) message is issued directing the gateway to set `single-dial-enable=no` for the call. The gateway will then resume call handling as if the call had just arrived from the PSTN, but prompt the caller to enter the destination telephone number (`single-dial-enable=no`) before continuing with call processing.

Static announcement branding

When the multiple logical gateway feature is enabled on a MultiVoice Gateway, MVAM, or a third party billing application, may select a set of voice announcements for playback from multiple sets of voice announcements stored on the gateway. This is known as *branding*.

S 912

By sending either an ARJ or ACF message, containing an announcement directory specifier, the gateway will playback voice announcements from the named directory on the pc-flash card for the current call.

Executing the branding instructions, the gateway will search for the voice announcement directory using the value assigned to the Voice-Ann-Dir parameter. When `voice-ann-dir=/current` (default), when MVAM requests a specific directory (brand) of announcements for a call, the gateway will search for those announcements starting in the /current directory. For example, if MVAM specified "italian", the gateway would search for announcements in the directory `/current/italian/`.

Note: It is recommended that only four "brands" of static announcements are used, due to limitations in the announcement cache size. Using more than four will degrade announcement quality and overall gateway performance.

Configurable call timers

This release of MultiVoice supports the use of configurable call timers, controlled by MVAM or a third party billing application, which support timed billing plans (such as: pre-paid phone cards, pre-paid cellular accounts).

Using an ACF message, MVAM or a third party billing application, set the following timers:

Timer	Description
Call countdown timer	This timer sets the time remaining before a gateway disconnects the current call. When this timer expires, the gateway will play an announcement that time has expired and disconnects the call. • By default, once the timer is set on the gateway, the `h323drq.au` announcement file is played back for the caller upon call termination • If the MVAM or third party billing application uses its own countdown timer, the announcement specifier in an Disengage Request (DRQ) massage may be used to select a different announcement file for playback upon call termination
Call disconnect warning timer	This timer specifies when a call disconnect warning announcement will be played for the caller. This announcement alerts the caller to the time remaining before this call is terminated. • By default, once this timer is set on the gateway, the `h323bkin.au` announcement file is played back for the caller when this timer expires • If the MVAM or third party billing application uses its own disconnect warning timer, the announcement specifier in an Interrupt Request (IRQ) massage may be used to select a different announcement file for playback when this timer expires

S 913

New Trunk and Call status reporting

Each MultiVoice Gateway reports its current call processing status as part of a Registration Request (RRQ) message to MVAM. This message includes data on trunk, trunk group and DS0 status. The initial RRQ message, sent to MVAM when a gateway is initialized, will contain a full report on all the trunks used by the physical gateway. The RRQ messages sent during keep-alive registration include only the status changes since the previous registration message.

H.323 call-specific administration messages

Call administration information is transmitted as part of the non-standard data included in registration, admission and status (RAS) messages exchanged between the gateway and gatekeeper for each call. This data consists of a set of parameters using URL encoding, as described in RFC 1738, with each parameter composed of a set of attribute value pairs.

This non standard data may include the following call administration information:

- ANI/CLID
- Conference identifier
- User PIN
- Inbound or outbound trunk identification
- Enable voice announcement playback
- Select voice announcement playback
- Internal call timer and disconnect timer settings
- Call failures
- Call results
- Trunk group and DS0 status information
- Available digital signal processors (DSPs)
- Maximum number of calls a MultiVoice Gateway may support

DS0 Status (in-service/out-of-service)

A MultiVoice Gateway reports trunk, trunk group, and DS0 information to MVAM for each trunk. This includes:

- Trunk group
- Physical address
- DS0 service status (in-service or out-of-service)

Note: A DS0 is in-service for a logical gateway when it belongs to the associated trunk group and is in the "up" state. Information regarding DS0 activity (in-use, free) is not reported via RRQ. This is handled separately. traced from the per-call trunk/DS0 reporting mentioned below.

Trunk groups and physical address (shelf, slot, etc.) information are provided to MVAM to allow dynamic tracking of DS0 activity and trunk group assignments, and provided for future support of DS0 selection by physical-address for outbound PSTN calls.

Full trunk and DS0 status reporting is performed only when necessary, enhancing gateway performance. Full RRQ's are used to report complete trunk and DS0 information, usually when a gateway is initialized or else when requested by MVAM. Lightweight RRQ's are used to

S 914

report only status changes for trunk and DS0 information. MVAM may request complete trunk and DS0 information by responding to a lightweight RRQ with a Registration Reject (RRJ) message containing a reject reason of `FullRegsitrationRequired`.

Note: Currently, trunk and DS0 status is not reported for BRI lines. Only the following information is reported for MultiVoice Gateways using BRI:

- Number of idle VOIP ports.
- value of maxCalls in VOIP profile.

Trunk and DS0 reporting (per call)

For each call processed by a MultiVoice Gateway, trunk group and physical address information for the DS0 connection are reported. This information is sent from the gateway to the gatekeeper as non-standard data in these registration, admission and status (RAS) messages, for the following call types:

Message	Call type	Trunk or DS0 information
Admission Request (ARQ)	Inbound (from PSTN)	The trunk group and physical address of the DS0 upon which the call arrived.
Bandwidth Request (BRQ)	Outbound (to PSTN)	The trunk group and physical address of the DS0 upon which the call went out.
Disengage Request (DRQ)	Inbound (from PSTN) and Outbound (to PSTN)	The physical address of the DS0. For outgoing PSTN calls, the trunk group or DS0 information may not be present.
Disengage Confirmation (DCF)	Inbound (from PSTN) and Outbound (to PSTN)	The trunk group and DS0 information for gatekeeper-initiated call terminations.

Trunk and DS0 selection (per call)

Currently, MultiVoice Gateways only support trunk-group based routing for outbound PSTN calls. To do this, using trunk groups must be enabled in the System profile of each gateway in the MultiVoice network. Each T1 must also be assigned a trunk group.

Note: Trunk groups should only be assigned at the T1 level.

The physical address information collected by the gateway for each DS0 is used currently by MVAM to dynamically track DS0 activity. It is currently not used for DS0 to DS0 linking. In the future, both trunk group and/or physical address information will be available for DS0 selection on the gateway. When this happens, trunk groups should only be used when processing both VoIP and data calls on the same gateway. Otherwise, only gatekeeper, physical-address based, DS0 routing should be used.

Usage: This feature is enabled or disabled by assigning either `Yes`, enabling processing of call-specific administration instructions, or `No` (default), reverting global administration of VoIP calls using the values set in the Voip { X X } profile.

The following example illustrates how to enable multiple logical gateway processing on this MAX TNT:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set gk-mlg-control=yes
admin> write
VOIP/{ 0 0 } written
```

Dependencies: This parameter has the following dependencies:

- If `gk-mlg-control=yes`, the value of Vpn-Mode defaults to `N/A`
- If `gk-mlg-control=yes`, the value of Single-Dial-Enable defaults to `N/A`
- Changes to this parameter are effective with the next VoIP call

Location: Voip { X X }

Configuring the H.245 pipeline signal model

By tying the H.323 Alert messaging to PSTN Alerting, the gateway conveys H.245 startup information on top of the Call Proceeding message. This creates a virtual inband pipeline for call signal processing by mapping PSTN actions into H.323 actions.

In all cases, the H.245 connection information is included in all H.323 messages (Call Proceeding, Alerting, and Connect). This enables a gateway to provide the support for the following inband messaging modes:

Inband messaging mode	Description
Early alerting	In this mode, the H.323 Call Proceeding message is sent upon receipt of the Admission Confirmation (ACF) from the gatekeeper, the H.323 Alerting message is sent upon receipt of WAN inband notification from the outdialed trunk, and an H.323 Connect message is sent up receipt of the PSTN Connect message.
Slow proceeding	In this mode, the H.323 Call Proceeding message is sent upon receipt of WAN inband notification from the outdialed trunk, an H.323 Alerting message is sent upon receipt of the PSTN Alerting message, and the H.323 Connect message is sent upon receipt of the PSTN Connect message.
Fast proceeding	In this mode, which is recommended for use over high latency links, the H.323 Call Proceeding message is sent upon receipt of the Admission Confirmation (ACF) message from the gatekeeper, an H.323 Alerting message is sent upon receipt of the PSTN Alerting message, and the H.323 Connect message is sent upon receipt of the PSTN Connect message.

Usage: The Signaling-Model parameter sets the inband messaging mode used by the gateway when mapping H.323 alert messaging and PSTN alerting, and accepts the following values.

Parameter value	Description
`early-alerting`	This value (default) enables inband call signal processing on a gateway using the Early Alerting inband messaging mode.
`slow-proceeding`	This value enables inband call signal processing on a gateway using the Slow Proceeding inband messaging mode.
`fast-proceeding`	This value enables inband call signal processing on a gateway using the Fast Proceeding inband messaging mode.

The following example illustrates how to change the default value of the Signaling-Model parameter.

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read

admin> set signaling-model=fast-proceeding

admin> write
VOIP/{ 0 0 } written
```

Dependencies: Changes made to the Signaling-Model parameter take effect with the next VoIP call.

Location: Voip { x x }

Enabling fax packet redundancy

Redundant packet data is defined as the last *n* packets transmitted appended to the current packet. The value of *n* is set through the CLI using the Packet-Redundancy parameter. Once defined, this parameter controls processing of several hundred milliseconds of packet jitter and allows the optional transmission of redundant packet data for fax calls across networks experiencing instances of packet loss and packet jitter.

Assigning the Packet-Redundancy parameter a value (such as, `packet-redundancy = 4`), will cause MAX TNT to append that number of previously sent packets onto the current packet. On networks experiencing measurable packet loss, this improves the reliability of the fax transmission.

Depending upon the amount of measurable packet loss for a network, the redundancy parameter should be set accordingly:

Network condition	Recommended value(s)
Packet loss occurs in frequent bursts.	1 - 5
Occasional packet loss (less than one percent)	0 (default)
Occasional packet loss (greater than one percent)	1 - 2

S 917

The additional bandwidth required for each fax call increases proportionally to the level of redundancy, adding 50 bytes of packet data per increment. To support this feature, MultiVoice requires Real-time fax support be enabled on the MultiVoice Gateway. This may be verified by checking the Base profile for the `rt-fax-enabled=yes` entry.

This enhancement uses a slip buffer to :

- Allow MultiVoice Real-time fax to tolerate packet jitter
- Keep the modem fed with data, preventing modem underrun

Fixed sized packet format

The packet redundancy scheme uses a fixed-size packet format, consisting of a 49-byte payload, a prefixed sequence number, and a length field which precedes the payload data. When packet redundancy is enabled, *n*-length payload pairs are added at the end of the packet; where *n* is the value of the Packet-Redundancy parameter. Previously, MAX TNT sent variable length packets that were guaranteed to be zero terminated; allowing Class 1 modems to underrun gracefully.

Usage: The Packet-Redundancy parameter accepts values from 0 through 5, directing MultiVoice to append the designated number of previously transmitted fax packets to the current packet, as follows:

Parameter value	Specifies
0	No change from the default packet behavior.
1	Append and send the previous fax packet with the current fax packet.
2	Append and send the two previous fax packets with the current fax packet.
3	Append and send the three previous fax packets with the current fax packet.
4	Append and send the four previous fax packets with the current fax packet.
5	Append and send the five previous fax packets with the current fax packet.

The following example illustrates how to change the default value of the Packet-Redundancy parameter.

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read

admin> set packet-redundancy=4

admin> write
VOIP/{ 0 0 } written
```

Dependencies: The following dependencies apply to this parameter:

- Once saved, packet redundancy is enabled with the next VoIP call
- This value is set to `N/A` when `fixed-packets=no`.